

CLAIMS

1. Method of access control to a secure area, particularly to a transport vehicle, in which a person who would like to access the secure area is asked for personal data, these personal data are written (100) on a card (300), this card (300) is issued for the attention  
5 of this person or given back to this person, and then at the time of access to the secure area, the personal data supplied by the person presenting this card are compared (200) with the personal data written on the card (300) to  
10 ensure that this person is actually the person authorised to use this card, method including two steps in which biometric readings (120, 220) are made directly on the person, one before the card is issued or given back (300) and the other at the access to the secure area, the  
15 recorded biometric data before the card is issued or given back (120) forming data written on the card (300), the biometric data recorded at the access to the secure area (220) being compared with the data on the card (300), characterised in that the biometric data are  
20 written on the card (300) at least partially using a non-graphic method (310).

2. Method according to claim 1, characterised in that the card (300) issued or given back comprises a memorising magnetic strip (310), and in that the  
25 biometric data are written on the card (300) by memory means on this magnetic strip (310).

3. Method according to claim 1 or claim 2, characterised in that it includes a step in which an identity check is made on the person making the record,  
30 using an identity document, at the same time as biometric

readings are made directly on the person, before the card is issued or given back (100).

4. Method according to any one of the previous claims, characterised in that biometric data are compared  
5 (210) at the access to the secure area (200) using computing means (210).

5. Method according to any one of the previous claims, characterised in that the biometric data (120, 220) comprise at least one fingerprint of the person.

10 6. Method according to any one of claims 1 to 4, characterised in that biometric data comprise data recorded on the eye of the person.

7. Method according to any one of claims 1 to 4, characterised in that biometric data comprise voice  
15 parameters of the person.

8. Method according to any one of claims 1 to 4, characterised in that biometric data comprise geometric parameters of the person's face.

9. Method according to any one of claims 1 to 4,  
20 characterised in that biometric data comprise geometric parameters of the person's hand.

10. Method according to any one of the previous claims, characterised in that the card is a supple boarding pass (ATB pass).

25 11. Method according to claim 10, characterised in that the card (300) issued or given back to the person is made of a material that can be torn off by the person, so that the person may easily destroy the biometric data written on the card (300).

30 12. Method according to any one of claims 1 to 9, characterised in that the card is a card made of plastic

material the same size as a credit card, comprising a magnetic strip on which biometric data are recorded.

13. Method according to any one of the previous claims, characterised in that a check-in desk is provided  
5 with means of routing luggage to the secure area, especially a transport vehicle, and with automatic means for reading biometric data (120) on a person, and also with means (110) for writing these biometric data on a card, so that the first biometric reading (100) is done  
10 at the same time as the person's luggage is checked in.

14. Method according to any one of the previous claims, characterised in that an access gate to the secure area is provided with a reading desk comprising a module (210) for automatically reading data written on  
15 the card (300) of a person wishing to access the secure area, a biometric sensor (220), and means (210) for automatically comparing biometric data recorded by the sensor (220) on the person and biometric data written on the card (300).

20 15. Module (200) for an automatic access control to a transport vehicle, comprising means (210) of automatically reading data recorded on an access card, characterised in that these read means (210) are designed to read biometric data registered on the card (300) in  
25 the form of text with no graphics, and in that the module (200) also comprises a sensor (220) for sampling biometric data on a person and means (210) of automatically comparing biometric data read on the card (300) with data recorded by the sensor (220), these  
30 comparison means being designed to indicate that data on the card and data provided by the sensor belong to a same person.

16. Access control assembly to a secure area, especially a transport vehicle, comprising means (110) of writing data onto cards controlling access to the secure area (300) on a first site, and means (200) of  
5 automatically reading such cards controlling access to the secure area (300) on a second site, the means on the first site (100) also include a sensor (120) for sampling biometric data on a person and means (110) of writing these data on a card controlling access to the secure  
10 area (300), and the means on the second site comprising automatic means (210) of reading biometric data written on the card (300), a sensor for sampling biometric data (220) on a person, and means of making an automatic comparison (210) between the biometric data read on the  
15 card (300) and the data read by this sensor (220), these comparison means being designed to indicate if the data on the card and the data on the sensor belong to the same person, characterised in that means on the first site (100) are intended for writing the biometric data on the  
20 card (300) using an at least partially non-graphic method.